

### **REMARKS**

Reconsideration of the above referenced application in view of the enclosed amendments and remarks is requested. This response corrects an informality in the Detailed Description, cancels claims 1-60, and enters new claims 61-94. Claims 61, 72, and 84 are the independent claims.

### **ARGUMENT**

The Office Action rejects claims 1-60 based on 35 U.S.C. § 102(e).

#### **35 U.S.C. § 102(e)**

The Office Action rejects claims 1-60 under 35 U.S.C. § 102(e) as being anticipated by U.S. patent no. 6,226,749 Marius M. Carloganu et al. (hereinafter "Carloganu"). Applicants respectfully submit that all of those rejections are improper. However, this response enters new claims to alter the focus of the claimed subject matter to some degree. To the extent that the rejections in the Office Action might be applied to any of the present claims, Applicants respectfully traverse.

Carloganu pertains to an apparatus for processing "secured commands" and "non-secured commands" (i.e., commands that have "either a secured command format ... or a non-secured command format") received from external devices. Specifically, according to Carloganu, "an application program running in an external device" sends non-secured and secured commands to "a secure processor" for execution. The secure processor "immediately executes" the non-secured commands, and the secured processor only executes secured commands if those commands pass tests for "authenticity" and "regularity." The secure processor determines which commands are secured and which are non-secured by looking up each received command in a "command set up table." (Abstract.)

By contrast, Claim 61 in the present application recites a processing system comprising (a) a processor that supports a normal execution mode and an "isolated execution mode," (b) memory to include an "isolated memory area" that is

inaccessible to the processor in the normal execution mode, and (c) storage to store a “processor executive (PE) handler” to be loaded into the “isolated memory area” during a boot process for the processing system. The PE handler is to “manage, from the isolated execution mode, at least one subsequent operation in the boot process.”

Carloganu has nothing to do with a processing system that supports “isolated execution mode” and “normal execution mode,” as recited in claim 61. Accordingly, Carloganu does not disclose memory to include an “isolated memory area” that is inaccessible to the processor in the normal execution mode, as recited in claim 61. *A fortiori*, Carloganu does not disclose storage to store at least part of a “PE handler to be loaded into the isolated memory area during a boot process for the processing system,” as recited in claim 61.

The Office Action asserts that column 4, lines 44-63 of Carloganu disclose a PE handler image to be loaded into an isolated memory area. However, that portion of Carloganu discloses no such thing. Instead, that portion of Carloganu discusses how “secured commands” and “non-secured commands” can have different formats, and how a “command set up table” can be used to distinguish between secured commands and nonsecured commands. Carloganu therefore does not anticipate claim 61 of the present application.

The other pending independent claims (i.e., claims 72 and 84) include features that are the same as or similar to the features discussed above with regard to claim 61, and the dependent claims inherently include the features of their respective parent claims. In addition, the independent and dependent claims recite numerous additional features that are not disclosed by Carloganu. For example, claim 76 recites the operation of “storing a thread count” to indicate “a number of threads operating in the isolated execution mode,” and claim 74 recites the operation of obtaining at least part of the PE handler from “PE handler storage” in a chipset of the processing system. For reasons including those set forth above, Carloganu does not anticipate any of pending claims of the present application.

Information Disclosure Statements

The Office Action includes a copy of an Information Disclosure Statement (IDS) that Applicants originally submitted on January 26, 2004. However, that copy does not include initials from the Examiner for the first six entries. Applicants respectfully request confirmation that the Examiner has considered all of the references listed on that IDS.

Also, at least one additional IDS has been recently submitted or is being submitted with this response. The Examiner may notice that some of the references from that IDS are also listed on an IDS or an eIDS that was considered by the Examiner on August 9, 2004, as evidenced by copies of an IDS and an eIDS that were included with the Office Action. However, it is unclear whether the Examiner considered those references in connection with the present application, as the copies received with the Office Action do not recite the serial number of the present application. Instead, those copies refer to patent application serial number 09/540,611. Applicants therefore respectfully request that the Examiner consider all of the references listed on the IDS, and that the Examiner provide Applicants with confirmation that those references have been considered.

09/540,613

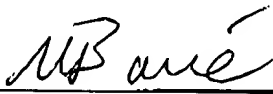
**CONCLUSION**

In view of the foregoing, claims 61-94 are all in condition for allowance. Applicants respectfully request reconsideration of the present application, consideration of any outstanding IDSs, and prompt issuance of a Notice of Allowance.

If the Examiner has any questions, the Examiner is invited to contact the undersigned at (512) 732-3927.

Respectfully submitted,

Dated: 11/5/04

  
\_\_\_\_\_  
Michael R. Barré  
Patent Attorney  
Intel Americas, Inc.  
Registration No. 44,023  
(512) 732-3927

c/o Blakely, Sokoloff, Taylor &  
Zafman, LLP  
12400 Wilshire Blvd.  
Seventh Floor  
Los Angeles, CA 90025-1026